ROUTING AND RECORD SHEET

P.R-2
1981

SUBJECT: (Optional)

ASIS Speech

FROM:	EXTENSION	NO.
Acting Chief, Policy and Plans 4-E-70 Headquarters		STAT
		DATE 20 AUG 1981

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DD/P&M	20 AUG 1981	8/20		Attached is a proposed topical outline for the use of the Director of Security in his presentation at the ASIS convention. It is the result of input from STAT and STAT SEG. I have also reviewed material in previous similar speeches and documents in the Registry. The STAT theme recurring from each of the above individuals is that they each felt that the topic of the lack of standardization is uppermost in the minds of the industrial security officers.
2. DDI OS	20 AUG 1981	21 AUG 1981		
3. DIOS	4 Sept 81		*	
4. [redacted]	SEP 1981			
5.				The outline is kept fairly general because of the audience that is expected. It must remain unclassified and some of the audience may not be familiar with the compartmented field.
6.				
7.				
8.				
9.				As a matter of information, approximately 25,000 people are expected at the seminar. From the Office of Security, [redacted] STAT are STAT expected to attend. I have some background data on some of these topics if desired.
10.				
11.				
12. * Howard - did the job.	Thanks, this			
13.			*	1 to 3 I think this is a lot to cover in 30 minutes.
14.				
15.				

STAT

FORM 1-79 610 USE PREVIOUS EDITIONS

Speech Before

THE AMERICAN SOCIETY FOR INDUSTRIAL SECURITY
New Orleans
2 September 1981

INTRODUCTION

I. The Threat

A. You have just heard an excellent presentation on the threat that is facing each of us in both government and industry.

B. It is real and ever present.

C. Neither the Intelligence Community nor industry can counter this threat alone. We must work together.

II. The Targets

A. Methods used by opposition to penetrate our security barriers are straightforward.

1. They seek out and exploit the weakest link.

B. They target:

1. Personnel vulnerabilities

2. Physical security breaches

3. Computer security weaknesses

III. CIA Security Program

A. Primary concern - Personnel Security

1. Our greatest asset, but also our greatest vulnerability is our people.

2. Sophisticated technical and physical security measures can afford us reasonable protection against the physical security threat, but people cannot be put under lock and key.

3. Numerous exploitable personnel weaknesses have been with us since Adam and Eve.

B. Our responsibility:

1. Counter the opposition effort.

2. Insure that we entrust our sensitive information to men and women of unquestioned loyalty to this country.

3. Our first line of defense - the integrity of our people.

4. It is here where we allocate the majority of our resources. If we fail in our personnel security program, all other security measures, physical-technical-industrial-operational-computer, are a waste of time.

C. CIA Personnel Security Program

1. Among the most comprehensive in Government.

2. It is manpower intensive, therefore, time-consuming and expensive, but it is necessary.

3. In addition to extensive field investigation, all staff employees undergo polygraph examination.

4. We have had our losses; Kampiles and Moore in Government and Boyce/Lee in the industrial area. We have learned from these losses and taken corrective measures. Some of you have felt the effect of this.

IV. Industrial Security Program

A. Government/Industry are Partners

1. I consider industry an integral part of our activities. They are so deeply involved, it is necessary to require similar security standards of industry participants.

2. Some industrial personnel are briefed in more depth on some highly classified programs than some of our own people.

3. Industrial contractor polygraph program working well.

4. Clearance processing takes time. We do the best we can, but require your help.

B. Pre-Screening

1. Our experience has been excellent.

2. Encourage you to use a comprehensive pre-screening mechanism. Talk to the candidates for clearances. Weed out the obvious problems before submitting them.

3. Do not expect us to screen employees for you.

4. Pre-screening, security education and employee counseling pay big dividends.

5. Know your people.

V. Standardization within Intelligence Community

A. Lack of standardization of Community Security policies, requirements and procedures is a major frustration within industry as it is in Government.

B. Community is sensitive to criticism and has made honest efforts to alleviate problems.

C. There has been progress, not as much as we would like.

D. Within the Intelligence Community, the DCI in his Community role, has established several standing committees. The Security Committee is one of these standing Committees.

E. The Security Committee strives to achieve standardization through a process of give and take. Each member agency has different concerns and problems.

F. Each small change in security procedures or standards has far reaching budget impact.

G. Where there is consensus and agreement, new procedures are given the force of policy by the DCI.

VI. Accomplishments to Date

A. Revised and updated uniform physical security standards governing construction and protection of facilities have been issued.

1. This is the first step to mutual acceptance of physical security inspections by various members of the community. It should ultimately result in a reduction of the physical security audits at contractor facilities by government agencies.

B. Community-wide Computer-assisted Compartmentation Control System (4C)

1. March 1982 is anticipated start-up date in the Washington area,

2. It will later be expanded within the U.S., then world-wide.

3. 4C will provide to NFIB users:

a. Real-time user certification of access

b. Real-time input and update capability

c. Data security through a password sign-on

d. Control of proprietary data

e. Updated audit trails and history file maintenance

f. Cleared facility data base

C. Standard non-disclosure agreement for government and industry. *

1. This new agreement solidifies the thrust of the SNEPP decision concerning pre-publication review.

* DDCI has not yet made a final decision on a standard form. We are recommending it now - should have response before 2 September.

D. Foreign Ownership, Control or Influence

1. Intelligence Community-wide policy established concerning contractors subject to foreign ownership, control or influence.

2. Contractors that fall in this category are generally ineligible for access to SCI activities and information.

E. Standardized Adjudication Procedures

1. Ensures common standards are applied throughout the Community on clearance adjudication criteria.

2. Adjudication seminars are being held with attendees from various agencies which provide for uniformity.

VII. Things Still to be Done

A. Uniform application of personnel security rules for SCI access.

1. DCID 1/14 establishes the personnel security criteria. It is under review for update.

2. Establishment of a uniform appeals procedure when SCI access is denied or revoked for cause.

3. Standardized Personal History Statement

a. Major problem area. Because of the wide use of the PHS and mechanisms already in place in certain agencies in support of their individual forms, changing to a standarized form would be significant budget impact. We are still working the problem.

4. Polygraph requirement for determining SCI access

a. Change to DCID 1/14 is under preliminary consideration to provide for some polygraph coverage before SCI access.

5. Need for greater cooperation among joint government users of industrial facilities to recognize each others facility inspections.

6. Automated Information Handling Systems

a. Dramatic increase in use of automated information handling systems has created a serious threat to operational security.

b. Proliferation of ADP systems in industry and their capability to store vast amounts of government classified information introduces greater demands on our security protection mechanisms.

c. Systems must be able to store multi-compartmented information, yet have safeguards to preserve the integrity of each program.

d. Rapidly advancing technology requires continued updating of security safeguards and thse changes must be uniform, yet flexible.